

FILED  
IN OPEN COURT

DEC - 2 2008

CLERK, U.S. DISTRICT COURT  
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA )  
                                  )  
                                  )  
v.                              )  
                                  )  
DANIEL ORJINTA              )  
                                  )  
                                  )  
Defendant                    )

Criminal No. 1:08CR483

**STATEMENT OF FACTS**

Were the United States to proceed to trial in this case, it would provide testimonial, documentary, and real evidence to prove beyond a reasonable doubt that, from no later than September 2007 through September 2008, in the Eastern District of Virginia and elsewhere, defendant DANIEL ORJINTA (the "Defendant") did unlawfully, willfully and knowingly agree, combine and conspire with others to execute and attempt to execute a scheme or artifice (i) to defraud a financial institution and (ii) to obtain moneys, funds and credit owned by and under the custody and control of a financial institution by means of materially false and fraudulent pretenses and representations in violation of Title 18, United States Code, Section 1349 (Bank Fraud). Specifically, the evidence would establish, at a minimum, the following facts:

1. Between approximately September 2007 and September 2008, Defendant, Tobechi Onwuahara (ONWUHARA), and others agreed to perpetrate a scheme to defraud financial institutions of substantial sums of money by fraudulently assuming the identities of account holders on existing home equity line of credit loans (HELOC), and causing financial institutions to transfer funds from those HELOC accounts to overseas bank accounts controlled by co-conspirators.

2. The conspirators carried out their fraudulent scheme by first identifying individuals who held large HELOC accounts, typically greater than \$200,000. To identify victims, the conspirators obtained lists of first and second mortgage borrowers from direct marketing companies that sold lists of sales leads for mortgage products. The conspirators obtained personal identifying information, including social security numbers, password clue information, and signature exemplars for victims from a variety of online sources. The conspirators also fraudulently obtained unauthorized access to potential victims' credit reports on publicly available credit report ordering websites to obtain information about potential victims' bank and HELOC accounts.

3. Once members of the conspiracy identified a target HELOC account and account holder and completed gathering personal identifying information about the target, certain members of the conspiracy called customer service contacts at target financial institutions and impersonated the HELOC account holders. To create the false appearance that the call originated from the HELOC account holders, the conspirators would use a caller id spoofing service to cause a false phone number to appear in the call recipient's caller identification display.

4. After providing the correct account information for a HELOC account holder, the fraudulent caller would first verify the unused balance on a HELOC account if the caller did not already know that information. Next, the caller would transfer funds out of the HELOC account and into a checking or savings account—although this was sometimes accomplished by logging into the victim's online account. Then, the caller would request a wire transfer of the funds to a foreign bank account controlled by members of the conspiracy. When a financial institution required written confirmations of wire transfer requests, the conspirators would request that the financial institution email or fax the wire transfer form to a free, web-based email account established by one or more

members of the conspiracy. Members of the conspiracy subscribed to a fax-to-web service that converted incoming faxes to a free web-based email account. The conspirators would then complete the wire transfer form and forge the HELOC account holder's signature based on exemplars obtained from loan documents and publicly-available, property-record databases. Additionally, the fraudulent caller would call the account holder's phone company and have the victim's home phone number forwarded to a pre-paid cell phone in the possession of one of the co-conspirators for a period of several hours in order to receive confirmation phone calls from the financial institution.

5. The Defendant provided overseas accounts to ONWUHARA. The conspirators would direct the wire transfers to be sent to these overseas bank accounts. The holders of the overseas accounts would keep a percentage of the fraudulently obtained proceeds and then cause the remainder of the proceeds to be transferred to accounts in Nigeria or the United States controlled by the U.S.-based members of the conspiracy. Portions of the illegally obtained proceeds would be shared among the persons who performed some role in the scheme.

6. As part of this fraudulent scheme, on or about December 7, 2007, ONWUHARA, impersonating the holder of a HELOC account with the United States Senate Federal Credit Union ("USSFCU"), called USSFCU's customer support in the Eastern District of Virginia, provided the account holder's personal account information, and fraudulently caused USSFCU to execute a wire transfer in the amount of \$280,000 dollars from Victim 1's account to a co-conspirator's bank account in Korea. The victim account holder resides in Alexandria, Virginia, which is in the Eastern District of Virginia.

7. On September 4, 2007, the Defendant sent information via email to ONWUHARA concerning a Bank of America account in the name of Southwest Equipment Sales Inc. ("BoA

Account") On September 9, 2007, ONWUHARA called State Farm Bank ("SFB") and requested a transfer of \$84,010 be sent from a victim account at SFB to the BoA Account. On September 10, 2007, conspirators sent an additional \$75,000 to the BoA Account. On November 21, 2007, the defendant again forwarded the BoA Account information via email. On November 23, 2007, conspirators transferred an additional \$650,500 into the BoA Account.

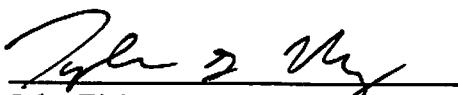
8. The Defendant admits that this statement of facts does not represent and is not intended to represent an exhaustive factual recitation of all the facts about which he has knowledge relating to the conspiracy to commit bank fraud as described herein.

9. The Defendant admits that his actions, as recounted herein, were in all respects intentional, knowing, and deliberate, reflecting an intention to do something the law forbids, and were not in any way the product of any accident or mistake of law or fact.

Respectfully submitted,

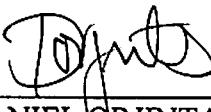
Dana J. Boente  
Acting United States Attorney

By:

  
John Eisinger  
Assistant United States Attorney

Tyler Newby  
Special Assistant United States Attorney

After consulting with my attorney and pursuant to the plea agreement entered into this day between the Defendant, DANIEL ORJINTA and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

  
\_\_\_\_\_  
DANIEL ORJINTA  
Defendant

I am DANIEL ORJINTA's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

  
\_\_\_\_\_  
David Smith  
Attorney for Daniel Orjinta

Date: 12/2/08